

AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

Claims 1 to 116 (Cancelled)

117. (New) A method comprising:

using a computer to generate a pruned attack tree, using the computer comprises:

designating a root node of the pruned attack tree, the root node representing a starting point of an attack; and

for a current node included in the pruned attack tree, connecting a resulting node having a first state and an edge having a first transition value to the current node if determined:

another edge having a second transition value does not connect an ancestor of the current node to another node having a second state equivalent to the first state; and

the second transition value is equal to the first transition value.

118. (New) The method of claim 117 wherein the pruned attack tree is a tree including n levels, the root node is at level 0, n being at least 0.

119. (New) The method of claim 118 wherein the first state represents at least one of: an attacker state including a host and an attacker access level on the host, and a network state.

120. (New) The method of claim 119 wherein the edge from the current node at a level x to the resulting node at a level $x+1$ represents an action while in the first state including a first attacker state corresponding to the current node resulting in the second state including a second attacker state.

121. (New) The method of claim 120 wherein the action exploits a vulnerability on a host in the network.

122. (New) The method of claim 120 wherein the first attacker state represents a first host and a first attacker access level on the first host, and the second attacker state represents at least one of: a second host and a second attacker access level on the second host, and the first host and a second attacker access level on the first host; and

wherein the second attacker access level represents at least one of: an increase in attacker privilege, an increase in attacker access, and an increase in attacker knowledge.

123. (New) The method of claim 117 wherein the current node is at a level n , and the ancestors of the current node are located at levels in the pruned attack tree at a level less than n .

124. (New) The method of claim 123 wherein the pruned attack tree is generated using a breadth first search technique in which nodes are added at an n th level prior to adding any node from level $n+1$.

125. (New) The method of claim 117 wherein computer attack paths for a network are represented using pruned attack trees, the pruned attack trees representing the computer attack paths originating from a unique starting point.

126. (New) The method of claim 117 wherein the root node is one of: from within a network and external to a network.

127. (New) The method of claim 122 wherein using the computer further comprises evaluating each action that exploits a vulnerability of a host in accordance with connectivity data.

128. (New) The method of claim 127 wherein the connectivity data, the each action, and the vulnerability are stored in a database.

129. (New) The method of claim 117 wherein using the computer further comprises:
determining which hosts in the network are equivalent forming a group; and
representing the group with a single host.

130. (New) The method of claim 117 wherein using the computer further comprises using
connectivity information to generate the pruned attack tree, the connectivity information
including a connection between two endpoints representing elements of a configuration of the
network.

131. (New) The method of claim 130 wherein the connectivity information includes
physical connectivity between network interfaces and logical connectivity through network
communications protocols.

132. (New) The method of claim 130 wherein the connection is associated with a path
including one or more hops.

133. (New) The method of claim 132 wherein the one or more hops is associated with at
least one of: a filtering rule, a translation rule, and an interface of a host in the network.

134. (New) The method of claim 132 wherein at least one of the endpoints is associated
with a vulnerability on the at least one endpoint.

135. (New) The method of claim 134 wherein the vulnerability has an associated action resulting in exploitation of the vulnerability.

136. (New) The method of claim 135 wherein the associated action is related to an entity representing at least one of: an attacker access level, attacker knowledge level, a change to a network state.

137. (New) The method of claim 117 wherein the pruned attack tree is used to determine an effect of preventing at least one action.

138. (New) The method of claim 137 wherein using the computer further comprises:
modifying the pruned attack tree in accordance with eliminating at least one action in connection with a vulnerability associated with the host producing a modified attack tree; and
evaluating the modified attack tree.

139. (New) The method of claim 117 wherein using the computer further comprises:
using connectivity data representing connectivity between pairs of endpoints in the network; and
automatically generating the connectivity data in accordance with at least one translation rule, at least one filtering rule, and network configuration information.

140. (New) The method of claim 139 wherein the at least one translation rule includes at least one of: an address translation rule and a port translation rule.

141. (New) The method of claim 139 wherein using the computer further comprises:
selecting at least one address of a starting point of a computer attack using at least one rule; and
determining a portion of the connectivity data using the at least one address.

142. (New) The method of claim 141 wherein the at least one rule includes at least one of a filtering rule and a translation rule.

143. (New) The method of claim 141 wherein the at least one address is used in the generating to represent an alternate connectivity of a host.

144. (New) The method of claim 141 wherein the at least one address is one of an address in accordance with a communications protocol and an address associated with the network.

145. (New) The method of claim 121 wherein using the computer further comprises using vulnerability data to determine at least one of: requirements for an action, an attacker state resulting from an action, and a network state resulting from an action,

wherein the requirements include a locality describing whether a vulnerability can be exploited remotely over a network or locally on a host, the resulting attacker state includes an effect describing an access level or privilege or knowledge after an exploit of a vulnerability, and the resulting network state includes a denial of service describing a loss of service on a host after an exploit of a vulnerability.

146. (New) An article comprising a machine-readable medium that stores executable instructions for generating a pruned attack tree, the instructions causing a machine to:

designate a root node of the pruned attack tree, the root node representing a starting point of an attack; and

for a current node included in the pruned attack tree, connecting a resulting node having a first state and an edge having a first transition value to the current node if determined:

another edge having a second transition value does not connect an ancestor of the current node to another node having a second state equivalent to the first state; and

the second transition value is equal to the first transition value.

147. (New) The article of claim 146 wherein the pruned attack tree is a tree including n levels, the root node being at level 0, n being at least 0.

148. (New) The article of claim 147 wherein the first state represents at least one of: an attacker state including a host and an attacker access level on the host, and a network state.

149. (New) The article of claim 148 wherein the edge from the current node at a level x to the resulting node at a level $x+1$ represents an action while in a first state including a first attacker state corresponding to the current node resulting in the second state including a second attacker state.

150. (New) The article of claim 149 wherein the action exploits a vulnerability on a host in the network.

151. (New) The article of claim 149 wherein the first attacker state represents a first host and a first attacker access level on the first host, and the second attacker state represents at least one of: a second host and a second attacker access level on the second host, and the first host and a second attacker access level on the first host wherein the second attacker access level represents at least one of: an increase in attacker privilege, an increase in attacker access, and an increase in attacker knowledge.

152. (New) The article of claim 146 wherein the current node is at a level n , and the ancestors of the current node are located at levels in the pruned attack tree at a level less than n .

153. (New) The article of claim 152, further comprising executable code that generates the pruned attack tree using a breadth first search technique in which nodes are added to the

pruned attack tree at an n th level prior to adding any node from level $n+1$ to the pruned attack tree.

154. (New) The article of claim 146 wherein computer attack paths for a network are represented using pruned attack trees, the pruned attack trees representing computer attack paths originating from a unique starting point.

155. (New) The article of claim 146 wherein the starting point is one of: from within a network and external to a network.

156. (New) The article of claim 151, further comprising instructions causing a machine to evaluate each action that exploits a vulnerability of a host in accordance with connectivity data.

157. (New) The article of claim 156, further comprising instructions causing the machine to store the connectivity data, the each action, and the vulnerability in a database prior to generating the pruned attack tree.

158. (New) The article of claim 146, further comprising instructions causing the machine to:

determine which hosts in the network are equivalent forming a group; and
represent the group with a single host.

159. (New) The article of claim 156 further comprising instructions causing a machine to use connectivity information to generate the pruned attack tree, the connectivity information including a connection between two endpoints representing elements of a configuration of the network.

160. (New) The article of claim 159 wherein the connectivity information includes physical connectivity between network interfaces and logical connectivity through network communications protocols.

161. (New) The article of claim 159 wherein the connection is associated with a path including one or more hops.

162. (New) The article of claim 161 wherein the one or more hops is associated with at least one of: a filtering rule, a translation rule, and an interface of a host in the network.

163. (New) The article of claim 159 wherein at least one of the endpoints is associated with a vulnerability on the at least one endpoint.

164. (New) The computer program product of claim 163 wherein the vulnerability has an associated action resulting in exploitation of the vulnerability.

165. (New) The article of claim 164 wherein the associated action is related to an entity representing at least one of: an attacker access level, attacker knowledge level, a change to a network state.

166. (New) The article of claim 146, further comprising instructions causing the machine to use the pruned attack tree to determine an effect of preventing at least one action.

167. (New) The article of claim 166, further comprising instructions causing the machine to:

modify the pruned attack tree in accordance with eliminating at least one action in connection with a vulnerability associated with the host producing a modified attack tree; and evaluate the modified attack tree.

168. (New) The article of claim 146 wherein connectivity data representing connectivity between pairs of endpoints in the network is used by the executable code that generates, and further comprising instructions causing a machine to: automatically generates the connectivity data in accordance with at least one translation rule, at least one filtering rule, and network configuration information.

169. (New) The article of claim 168 wherein the at least one translation rule includes at least one of: an address translation rule and a port translation rule.

170. (New) The article of claim 168, further comprising instructions causing the machine to select at least one address of a starting point of a computer attack using at least one rule; and determine a portion of the connectivity data using the at least one address.

171. (New) The article of claim 170 wherein the at least one rule includes at least one of a filtering rule and a translation rule.

172. (New) The article of claim 171 wherein the at least one address is used in the generating to represent an alternate connectivity of a host.

173. (New) The article of claim 172 wherein the at least one address is one of an address in accordance with a communications protocol and an address associated with the network.

174. (New) The article of claim 146, further comprising instructions causing the machine to use vulnerability data to determine at least one of: requirements for an action, an attacker state resulting from an action, and a network state resulting from an action,

wherein the requirements include a locality describing whether a vulnerability can be exploited remotely over a network or locally on a host, the resulting attacker state includes an

Applicants : Lippmann et al.
Serial No. : 10/734,083
Filed : December 11, 2003
Page : 14 of 18

Attorney's Docket No.: MIT-186PUS

effect describing an access level or privilege or knowledge after an exploit of a vulnerability, and the resulting network state includes a denial of service describing a loss of service on a host after an exploit of a vulnerability.